(19) Europäisches Patentamt
European Patent Offic
Office européen des brevets

(11) EP 0 920 057 A2

# (12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
**02.06.1999 Bulletin 1999/22**

(51) Int. Cl.[6]: **H01L 23/58**, G11C 7/00

(21) Application number: **99102130.4**

(22) Date of filing: **04.01.1990**

(84) Designated Contracting States:
**BE CH DE DK ES FR GB LI NL SE**

(30) Priority: **12.01.1989 US 297472**

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
**90300090.9 / 0 378 306**

(71) Applicant:
**General Instrument Corporation**
**Horsham, Pennsylvania 19044 (US)**

(72) Inventors:
- **Gilbert, Robert C**
  **San Diego, California 92131 (US)**
- **Knowles, Richard M**
  **San Diego, California 92126 (US)**
- **Moroney, Paul**
  **Cardiff-By-Sea, California 92007 (US)**
- **Shumate, William allen**
  **San Diego, California 92116 (US)**

(74) Representative:
**Blatchford, William Michael et al**
**Withers & Rogers**
**Goldings House,**
**2 Hays Lane**
**London SE1 2HW (GB)**

## (54) Secure integrated chip with conductive shield

(57) A chip includes a secure section 11 having a fuse element 56 and a fuse altering device 58. A predetermined data pattern is formed by wiring and inverters 62 connected between an erasable memory 52 and an AND gate 60. An enabling circuit 55 allows the predetermined data pattern to be written into the memory 52 when an appropriate control signal is received at a terminal 63. The state of the fuse element 56 is then irreversibly altered by the fuse altering device 58 so that the predetermined data pattern in the memory 52 cannot be changed. After final pressing and packaging, secure data may be stored in a secure memory M since the data pattern in the memory 52 is the same as that in the inverters 62. Once the secure data is stored, an erase signal is provided to terminal 66 which thereby erases the memory 52. The contents of the secure memory M are thereafter unalterable.

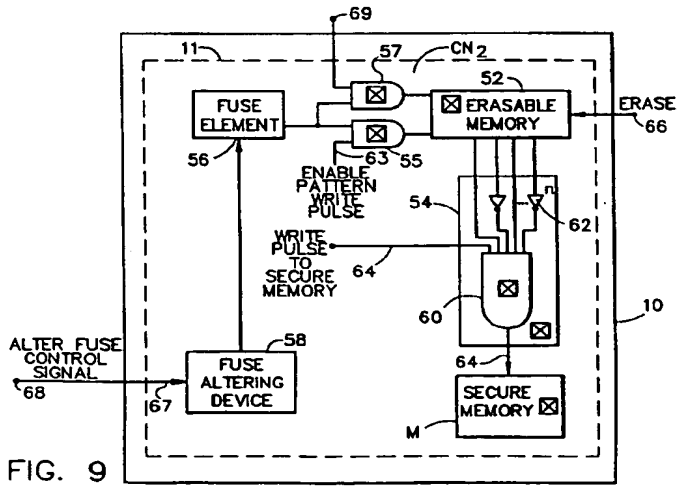


FIG. 9

EP 0 920 057 A2

## Description

**[0001]** The present invention generally pertains to integrated circuit chips for electronic data processing systems and is particularly directed to preventing inspection and/or modification of secure data that is stored or processed within a secure area of an integrated circuit chip.

**[0002]** Integrated circuit chips that process and store secure data include a secure area containing circuit elements for processing and storing the secure data, and a non secure area containing circuit elements for processing and storing non secure data and control signals. An integrated circuit chip contains a semi-conductive layer containing diffusions defining circuit element components; and a first conductive layer coupled to the semi-conductive layer to interconnect the components to thereby define the circuit elements. All modern integrated circuit chips include one or more conductive layers, typically for interconnecting circuit elements and components thereof. Generally these layers are used for both control signal and power signal distribution in a way that is intended to maximise signal interconnection density and reduce the area required for such interconnections.

**[0003]** The secure area further contains circuit elements for transferring non secure data and control signals to a data bus within the secure area for processing with the secure data by data processing circuit elements within the secure area. Logic circuit elements within the secure area enable the nonsecure data and the control signals to be transferred between the non secure area and the data bus within the secure area in response to control signals generated by the data processing circuit elements within the secure area.

**[0004]** Nevertheless, even though the secure data cannot be readily transferred in such an integrated circuit chip from the secure area to the non secure area, it is possible to gain access to secure data stored or being processed within the secure area by inspecting the secure area with such diagnostic tools as a scanning electron microscope (SEM) or a probe that couples an oscilloscope to a given node within the secure area from which the secure data can be accessed. Also, by delivering appropriate control signals to the logic circuit elements within the secure area by such means as a probe, it may be possible to cause the logic circuit to enable transfer of secure data to the nonsecure area from a data bus within the secure area that carries both nonsecure and secure data for processing by the data processing circuit elements within the secure area or to enable the secure data stored within the secure area to be replaced by clandestine data that would enable the intended security of the chip to be compromised.

**[0005]** The present invention provides an integrated circuit chip containing a secure area in which secure data is processed and/or stored, comprising:

a semiconductor layer containing diffusions defining circuit element components;

a first conductive layer coupled to the semiconductor layer to interconnect the components to thereby define circuit elements for distributing, storing, processing and/or affecting the processing of secure data;

a second conductive layer overlying the circuit elements to thereby define a secure area in which the circuit elements are shielded from inspection, and coupled to the circuit elements for conducting to the circuit elements a predetermined signal that is essential to an intended function of the circuit elements, whereby removal of the second conductive layer will prevent the predetermined essential signal from being provided to the circuit elements and thereby prevent the intended function;

characterised in that the shielded circuit elements further comprise:

a fuse element having an initial state and an irreversibly altered state; and

means coupled to the fuse element for irreversibly altering the state of the fuse element in response to a predetermined control signal;

wherein the fuse element is coupled to another component of the chip such that irreversibly altering the state of the fuse element prevents some function of the chip.

**[0006]** The invention will now be described by way of example with reference to the drawings in which:-

Figure 1 is a block diagram of an integrated circuit chip to which the present invention can be applied;

Figure 2 is a cross-sectional view illustrating the shielding of MOS circuit element components in the Figure 1 integrated circuit chip;

Figure 3 is a plan view illustrating the use of an overlying conductive layer to shield circuit element components and to conduct a predetermined signal to shielded MOS circuit elements;

Figure 4 is a cross-sectional view illustrating the shielding of bipolar circuit element components in an integrated circuit chip;

Figure 5 is a cross-sectional view illustrating the use of an overlying conductive layer to shield circuit elements and to conduct power to the shielded circuit elements;

Figure 6 is a block diagram illustrating an alterna-

tive topology for shielding a plurality of volatile memories;

Figure 7 is a plan view illustrating the use of an overlying conductive layer to carry a signal essential to the function of a circuit element;

Figure 8 is a block diagram of a system in the secure area of the chip for preventing the alteration of secure data stored in a predetermined memory location in accordance with the present invention;

Figure 9 is a block diagram of an alternative embodiment of a system in the secure area of the chip for preventing the alteration of secure data stored in a predetermined memory location; and

Figure 10 is a block diagram of a system in the secure area of the chip for limiting when the secure area may be accessed for testing.

**[0007]** Referring to Figure 1, a preferred integrated circuit chip 10 with which the present invention may be used includes a secure area 11 and a non secure area 12. The chip 10 is a VLSI (Very Large Scale Integrated) circuit chip. Within the secure area 11, the chip 10 defines the following circuit elements: a microprocessor 14 for processing secure data, a plurality of memories $M_1$,$M_2$,$M_n$ for storing secure data, a secure data bus 16, a secure address bus 17, transfer logic circuits 18, and secure clock and power control circuits 20. The chip 10 need not be limited to such a specific mixture of circuit elements, but may contain any mixture of circuit elements wherein secure data is to be either protected against unauthorised attacks of reading out or modification of secure data and/or instructions. The memories $M_1$, $M_2$, $M_n$ can be of any type, to wit: RAM (random-access memory), ROM (read-only memory), EPROM (electrically programmable ROM) EEPROM: (electrically erasable programmable ROM) and others, such as register files, FIFO (first-in/first-out) buffers, etc.

**[0008]** A conductive layer $CN_2$ covers the circuit elements 14, $M_1$, $M_2$, $M_n$, 16, 17, 18, 20 to shield such circuit elements from inspection, and thereby defines the secure area 11.

**[0009]** Within the non secure area 12, the chip 10 defines the following circuit elements. a memory 24, a logic circuit 26 and a nonsecure data bus 28.

**[0010]** In a chip 10 including MOS circuit elements, as illustrated in Figures 2 and 3, the chip includes a semiconductive substrate layer SC, a first dielectric layer $DE_1$, a first conductive layer $CN_1$, a second dielectric layer $DE_2$, a second conductive layer $CN_2$, an nth dilectric layer $DE_n$ and an nth conductive layer $CN_n$. Diffusions S and D in the semiconductive substrate layer SC define sources and drains, which are combined with gate conductors G and interconnected by the first conductive layer $CN_1$, to define complementary MOS field effect transistors that are arrayed to define the circuit elements of the chip 10. The first conductive layer $CN_1$, is coupled to a source S and a drain D by conductive contacts 30 through holes in the first dielectric layer $DE_1$. The second conductive layer $CN_2$ is coupled to the first conductive layer $CN_1$, by a contact 31 through a hole in the second dielectric layer $DE_2$ for conducting to the circuit elements a predetermined signal that is essential to an intended function of the shielded circuit elements.

**[0011]** Removal of the second conductive layer $CN_2$ will prevent the predetermined essential signal from being provided to the circuit elements and thereby prevent the intended function. The second conductive layer $CN_2$ overlies the circuit elements to thereby define the secure area 11 in which the circuit elements are shielded from inspection.

**[0012]** In a chip 10 including bipolar elements, as illustrated in Figure 4, the chip includes a semiconductive substrate layer SC, a first dielectric layer $DE_1$, a first conductive layer $CN_1$, second dielectric layer $CN_1$, an nth dielectric layer $DE_n$, and an nth conductive layer $CN_n$. Diffusions C, B and E in the semiconductive layer SC define collectors, bases and emitters which are interconnected by the first conductive layer $CN_1$, to define bipolar transistors that are arrayed to define the circuit elements of the chip 10. The first conductive layer $CN_1$, is coupled to a collector C and a base B by conductive contacts 32 through holes in the first dieletric layer $DE_1$ for conducting to the circuit elements a predetermined signal that is essential to an intended function of the shielded circuit elements. The second conductive layer $CN_2$ is coupled to the first conductive layer $CN_1$, by a contact 33 through a hole in the second dielectric layer $DE_2$ for conducting to the circuit elements a predetermined signal that is essential to an intended function of the shielded circuit elements.

**[0013]** Removal of the second conductive layer $CN_2$ will prevent the predetermined essential signal from being provided to the circuit elements and thereby prevent the intended function. The second conductive layer $CN_2$ overlies the circuit elements to thereby define the secure area 11 in which the circuit elements are shielded from inspection.

**[0014]** All circuit elements of the chip 10 that distribute, store, process or affect the processing of secure data utilise conductive layers, such as the interconnect layer $CN_1$, that are fabricated before and lie under the conductive layer, such as layer $CN_2$, which functions as a shield and thereby defines the boundaries of the secure area 11.

**[0015]** The second conductive layer $CN_2$ acts both as a shield to mechanical and SEM probing and as a predetermined essential signal carrying layer that cannot be removed without rendering the underlying circuit elements inoperable. The predetermined essential signal may be either a power signal or a control signal, such as an instruction. When the predetermined essential signal

is a power signal, removal of the shield layer $CN_2$ by either mechanical, chemical or other means for inspection purposes will then remove power from the underlying circuit elements, rendering them inoperable and also possibly forcing the same circuit elements to lose any data or logic state stored therein.

**[0016]** The technique is particularly effective for protecting secure data stored in a volatile memory, such as a volatile RAM. In an embodiment of the chip 10 in which the memories $M_1$ and $M_2$ are volatile memories, each of such memories $M_1$, $M_2$ is covered by the second conductive layer $CN_2$ to shield the memories $M_1$, $M_2$ from inspection; and a power signal is separately distributed to each of the memories $M_1$, $M_2$ from the portion of the second conductive layer $CN_2$ that overlies the respective memory $M_1$, $M_2$. Such distribution is shown in Figure 5, wherein the second conductive layer $CN_2$ is connected by a contact 34 to the source S of a transistor included in a volatile memory for providing power to the memory. Removal of the overlying portion of the second conductive layer $CN_2$ to enable inspection of the respective memory $M_1$, $M_2$ results in power being removed from the respective memory $M_1$, $M_2$. Since the memory $M_1$, $M_2$ is volatile, removal of power therefrom results in deletion of the secure data stored therein. Accordingly, an attempt to inspect the contents of either of the memories $M_1$, $M_2$ by removing only the portion of the second conductive layer $CN_2$ that overlies such memory will be unavailing.

**[0017]** In an alternative arrangement shown in Figure 6, power signals $V_{CC}$ are distributed from the second conductive layer $CN_2$ to a plurality of volatile memory elements M in a manner that takes up less space than in the embodiment described above, in which power is separately distributed to each of the memory elements M from only that portion of the second conductive layer as overlies such memory element M. In this arrangement each row of memory elements M receives power from the overlying second conductive layer $CN_2$ via a separate underlying first conductive layer $CN_1$. The second conductive layer $CN_2$ is connected to the respective first conductive layer $CN_1$ by conductive contacts 35. Although this arrangement does trade off some security for area efficiency, an attempt to inspect these memory elements M without causing the data to be deleted by a power loss resulting from removal of the second conductive layer $CN_2$ would require very high resolution removal of the second conductive layer $CN_2$ while leaving intact all interlayer conductive contacts 35 and the portion of the second conductive layer $CN_2$ that distributes power to these contacts 35.

**[0018]** Any combination of conductive layers may be used in this arrangement. The use of the conductive layers most highly embedded within the vertical dimension of the chip as the shielding conductive layers results in the greatest security.

**[0019]** Referring again to Figure 1, within the non secure area 12, the logic elements 26 and the memory 24 process and store nonsecure data and control signals. The non secure data and control signals are transferred from the nonsecure data bus 28 to the secure data bus 16 in the secure area 11 by the transfer logic circuit 18. The transfer logic circuit 18 transfers the nonsecure data and control signals to the secure data bus 16 within the secure area 11 for processing with the secure data by the microprocessor 14. The transfer logic circuit 18 enables the nonsecure data and the control signals to be transferred between the non secure data bus 28 and the secure data bus 16 in response to control signals generated by the microprocessor 14 that indicate when nonsecure data is present on the secure data bus 16. The microprocessor 14 monitors the status of the data signals on the secure data bus 16, and generates the control signals that enable the logic circuit 18 to transfer data signals and control signals between the nonsecure data bus 28 and the secure data bus 16 only during such times as nonsecure data is present on the secure data bus 16.

**[0020]** As described above, the conductive layer $CN_2$ overlies the transfer logic circuit 18 in order to shield the transfer logic circuit from inspection. The conductive layer $CN_2$ also conducts a power signal to the transfer logic circuit 18, whereby removal of the conductive layer $CN_2$ for the purpose of inspecting the transfer logic circuit 18 results in power being removed from the transfer logic circuit 18 and prevents the logic circuit 18 from transferring any data or control signals between the secure data bus 16 and the nonsecure data bus 28. Likewise, removal of the conductive layer $CN_2$ in order to allow control signals to be delivered to the transfer logic circuit 18 by such means as a probe for enabling secure data to be transferred from the secure area 11 to the non secure area 12 of the chip 10 will be unavailing since such removal of the shielding conductive layer $CN_2$ also removes power from the transfer logic circuit 18.

**[0021]** This technique may be extended in the reverse direction, so that clandestine data cannot be written into a secure memory $M_1$, $M_2$, $M_n$ from the non secure area 12. The microprocessor 14 provides memory access logic circuit, which enables data on the secure data bus 16 to be stored in the memories $M_1$, $M_2$, $M_n$; and the shielding conductive layer $CN_2$ conducts a power signal to the microprocessor 14. Thus removal of the shielding conductive layer $CN_2$ in order to deliver control signals to the memory access logic circuit of the microprocessor 14 that would enable clandestine data to be substituted in the memories of $M_1$, $M_2$, $M_n$ for the secure data to thereby compromise the intended security of the chip would be unavailing since removal of the shielding conductive layer $CN_2$ removes power from the microprocessor 14 and thereby prevents the memory access logic circuit therein from enabling data to be stored in the memories $M_1$, $M_2$, $M_n$.

**[0022]** In one example each of the shielding logic circuits 14, 18 in the secure area is separately coupled to

only that portion of the shielding conductive layer $CN_2$ that overlies such logic circuit 14, 18 for receiving a power signal from only that overlying portion of the shielding conductive layer $CN_2$.

**[0023]** In an example shown in Figure 7, a secure signal is distributed in a conductive layer $CN_1$, that underlies layers $CN_2$ and $CN_n$, and shielding signals (such as essential control or power signals) are distributed in the overlying shield layers $CN_2$ and $CN_n$, respectively. The boundaries of one shielding conductive layer $CN_n$, are shown in the drawing by solid lines, the boundaries of the other shielding conductive layer $CN_2$ are shown in the drawing by dashed lines, and the underlying conductive layer $CN_1$ is shown in the drawing by shading. The underlying conductive layer $CN_1$ is entirely shielded by either one or the other of the shielding conductive layers $CN_2$ and $CN_n$ and one portion of the underlying conductive layer $CN_1$ is shielded by both of the shielding conductive layers $CN_2$ and $CN_n$.

**[0024]** An attempt at cutting through the shield layers $CN_2$ and $Cn_n$ with chemicals or conventional lasers or microprobes to gain access to the secure signal in the conductive layer $CN_1$ results either in the conductive layer $CN_1$ becoming connected (shorted) to the shield layers $CN_2$ and $CN_n$ or in an open circuit being created in the circuit paths defined by the conductive layers $CN_1$, $CN_2$, $CN_n$, which thereby disrupts distribution of the secure signal and the essential signals and alters the intended functions of the circuit elements connected to the conductive layers $CN_1$, $CN_2$ and $CN_n$ so as to impair the intended function of the chip 10.

**[0025]** It is critically important that certain secure data stored in the chip 10 during formation of a product that includes the chip not be modified after the storage of such secure data. To accomplish this purpose the chip 10 includes a system for preventing the alteration of secure data stored in a predetermined memory location. Alternative embodiments of such a prevention system are shown in Figures 8 and 9.

**[0026]** The system of Figure 8 includes a memory M, a memory control logic circuit 38, a decoder 40, a fuse element 42 and a fuse altering device 44. This system is applicable to and includes as the memory M, each of the memories $M_1$, $M_2$, $M_n$ in which secure data is stored.

**[0027]** The memory M has a plurality of memory locations, with a predetermined location being for the storage of unalterable secure data from the data bus 16.

**[0028]** The memory control logic circuit 38 is coupled to the memory M by an address bus 46 for causing data to be stored in locations of the memory M indicated by address signals provided on the address bus 46 when a "write" signal is provided on line 47 from the memory control logic circuit 38 to the secure memory M.

**[0029]** The fuse element 42 has an initial state and an irreversibly altered state. The term "fuse element" refers to both fuses and antifuses. Fuse elements are formed in the chip 10 by the combination of a metallic conductive layer and a polysilicon conductive layer. Antifuse elements can be formed in the chip by metallic conductive layers, polysilicon conductive layers or a combination of both. Antifuse elements are formed by $P^+/N^+$ semiconductor junction diodes and $P^-.N^-$ semiconductor junction diodes formed in a semiconductive layer of the chip by conductor/oxide conductor structures or by conductor/amorphous silicon/conductor structures in the chip.

**[0030]** The fuse altering device 44 is coupled to the fuse element 42 for irreversibly altering the state of the fuse element 42 in response to a predetermined control signal received on line 48 from a terminal 50 that is external to the secure area 11. Alternatively, the control signal on line 48 is received from a terminal (not shown) that is internal to the secure area 11.

**[0031]** The decoder 40 is coupled to the fuse element 42, the memory control circuit 38 and the address bus 46 for monitoring the state of the fuse element 42 and the address signals on the address bus 46, and for preventing the memory control circuit 38 from causing data to be stored in the predetermined memory location of the memory M after the state of the fuse element 42 has been altered irreversibly whenever the predetermined memory location is indicated by an address signal on the address bus 46.

**[0032]** The second conductive layer $CN_2$ shields the memory M, the memory control logic circuit 38, the decoder 40, and the fuse element 42 from direct external access.

**[0033]** The memory M, the memory control logic circuit 38 and the decoder 40 are all coupled to the second conductive layer $CN_2$ so as to be powered by the power signal carried by the second conductive layer $CN_2$.

**[0034]** The system of Figure 8 is used to prevent the alteration of secure data initially stored in the predetermined locations of the memory M. Once the state of the fuse element 42 is irreversibly changed, the decoder 40 prevents the writing of any further data into the predetermined memory locations indicated by the address signals on the address bus 46.

**[0035]** The fuse element 42 in the system of Figure 8 also may be connected to other shielded circuit elements (not shown) that perform or affect certain preliminary secure data processing functions that are applicable only prior to such time as the product that includes the chip is distributed to users of the product, such as preliminary processing of the secure data or the loading of instructions for processing the secure data. Means, such as the decoder 40, are coupled to the fuse element 42 and such other shielded circuit elements for monitoring the state of the fuse element and for preventing the intended function of such other shielded circuit element after the state of the fuse element has been altered irreversibly.

**[0036]** Many fuse technologies allow fusing only at a foundry during the secure integrated circuit chip fabrication process. For example, certain foundries may

require that an oxide be grown over a polysilicon (or other fuse material) after the fuse has been blown to afford better long term device reliability. The system of Figure 9 allows a separate manufacturer to load secure data into the secure memory M after foundry fusing, yet still prevents alteration of the contents of the memory M.

**[0037]** The system of Figure 9 includes a memory M, an erasable memory 52, such as an EPROM or an EEROM (electrically erasable ROM), memory control logic circuit 54, an enabling circuit 55, a fuse element 56, an AND gate 57 and a fuse altering device 58. The memory control logic circuit 54 includes an AND gate 60, and N connections including wiring and inverters 62 that couple the AND gate 60 to the erasable memory 52. The inverters 62 are connected between selected inputs to the AND gate 60 and selected memory locations in the erasable memory 52 so as to define a predetermined data pattern in the erasable memory 52 that must be present to enable the AND gate 60.

**[0038]** The memory M has a plurality of memory locations, with a predetermined location being for the storage of unalterable secure data.

**[0039]** The enabling circuit 55 enables a data pattern to be stored in the erasable memory 52 when a write enable signal is applied on line 63 to the enabling circuit 55.

**[0040]** The memory control logic circuit 54 couples the memory M to the erasable memory 52 in such a manner as to cause data to be stored in the predetermined location of the first memory M in response to a write signal on line 64 to the AND gate 60 whenever the erasable memory 52 contains a predetermined data pattern.

**[0041]** The contents of the erasable memory 52 may be erased by providing an "erase" control signal at an erase terminal 66 located outside the secure area 11 of the chip 10.

**[0042]** The fuse element 56 has an initial state and an irreversibly altered state. The fuse altering device 58 is coupled to the fuse element 56 for irreversibly altering the state of the fuse element 56 in response to a predetermined control signal received on line 67 from a terminal 68 that is external to the secure area 11. Alternatively, the control signal on line 67 is received from a terminal (not shown) that is internal to the secure area 11.

**[0043]** A data pattern is provided at a data terminal 69 and fed into the erasable memory through the AND gate 57. The AND gate 57 has one input connected to the fuse element 56 so as to enable data to be written into the erasable memory 52 only while the fuse element 56 is in its initial state.

**[0044]** The fuse element 56 also is coupled to the enabling circuit 55 so as to enable the predetermined data pattern to be stored in the erasable memory 52 only prior to the state of the fuse element 56 being irreversibly altered.

**[0045]** N bits of erasable memory 52 are required. At the foundry, the predetermined pattern of ones and zeros corresponding to the pattern of inverters 62 coupling the erasable memory 52 to the AND gate 60 is loaded into the erasable memory 52 to enable the AND gate 60 to pass a "write" control signal on line 64 to the memory M. After the predetermined pattern of ones and zeros is loaded into the erasable memory 52, the state of the fuse element is irreversibly altered so that the predetermined pattern cannot be changed. At this point, processing and packaging of the integrated circuit chip 10 can continue, subject to the condition that the final processing and packaging steps do not disturb the stored predetermined pattern in the erasable memory 52.

**[0046]** After the chip 10 is shipped to a separate manufacturer, secure data can be stored in the secure memory M since the predetermined pattern stored in the erasable memory 52 matches the predetermined pattern hard-wired into the memory control logic circuit 54 by the inverters 62.

**[0047]** Once the secure data is stored in the secure memory M, an "erase" signal is applied to the erase terminal 66 to erase the contents of the erasable memory 52 and thereby prevent alteration of the secure data stored in the secure memory M.

**[0048]** The second conductive layer $CN_2$ shields the memory M, the erasable memory 52, the memory control logic circuit 54, the enabling circuit 55 and the fuse element 56 from direct external access.

**[0049]** This technique makes the system of Figure 9 secure from any attack short of an extremely precise X-ray beam or other complex means that may be used to remotely reprogram the erasable memory 52 through the covering layers of the chip 10. The security of this technique relies on the fact it is difficult to remotely reprogram the contents of an EEROM or EPROM, or to reconnect a blown fuse element. If a high power unfocused or diffuse X-ray or other means could essentially randomise the EEROM or EPROM contents, then an attacker could make repeated attempts to achieve the enabling pattern. Thus, security may also require that the EEROM or EPROM cells be designed to be biased in terms of their state, in other words, biased towards a preferred pattern of all ones or all zeros. Thus any unfocused beam would with high probability drive the contents to the preferred pattern rather than to the predetermined pattern that enables data to be stored in the memory M. Security can also be increased by using a longer predetermined pattern, with a larger number N of bits.

**[0050]** The memory M, the erasable memory 52, the AND gate 60 and the enabling circuit 55 are all coupled to the second conductive layer $CN_2$ so as to be powered by the power signal carried by the second conductive layer CN2.

**[0051]** The fuse element 56 in the system of Figure 9 also may be connected to other shielded circuit elements (not shown) that perform or affect certain preliminary secure data processing functions that are

applicable only prior to such time as the product that includes the chip is distributed to users of the product, such as preliminary processing of the secure data or the loading of instructions for processing the secure data. The fuse element 56 is coupled to such other shielded circuit element so as to enable the intended function of such other shielded circuit element only prior to the state of the fuse element being irreversibly altered.

**[0052]** The secure data alteration prevention systems of Figures 8 and 9 are the subject of a commonly assigned patent EP-A-0378307 filed 4 January 1990, entitled "Prevention of Alteration of Data Stored in Secure Integrated Circuit Chip Memory".

**[0053]** Manufacturing of complex integrated circuit chips requires complete access to the internal circuit elements during testing operations to insure that all included circuit elements work correctly. However, high accessibility for testing purposes generally is a security weakness for chips containing secure data or data which should not be modified.

**[0054]** Figure 10 shows a system for permanently disabling test signal paths after testing operations are completed, so that no further access to internal secure circuit elements from the external pins of the chip is possible. This system includes a fuse element 70, first and second inverters 72, 74, a resistance 75, first and second NAND gates 76, 78 and a fuse altering device 79.

**[0055]** The fuse element 70 has a initial state and an irreversibly altered state. The fuse altering device 79 is coupled to the fuse element 70 for irreversibly altering the state of the fuse element 70 in response to a predetermined control signal received on line 80 from a terminal 81 that is external to the secure area 11. Alternatively, the control signal on line 80- is received from a terminal (not shown) that is internal to the secure area 11.

**[0056]** The fuse element 70 is coupled to the first and second NAND gates 76, 78 so as to enable the secure areas of the chip 10 to be accessed for testing only prior to the state of the fuse element 70 being irreversibly altered.

**[0057]** The fuse element 70 and the inverters 72, 74 are connected in series to one input to the first NAND gate 76. The output of the first NAND gate 76 is applied to an external test data output terminal 82.

**[0058]** The fuse element 70 and the inverters 72, 74 are also connected in series to one input to the second NAND gate 78.

**[0059]** The second NAND gate 78 passes a test command signal from an internal test command input terminal 84 to a test command input node 86 within the secure area 11 of the chip 10. Test data is provided at internal test data output node 88 within the secure area 11 of the chip 10 in response to a test command input signal being provided to the internal test command input node 86. The test data provided at the internal test data output terminal may be accessed from the secure circuit elements of the chip 10, such as the circuit elements 14, $M_1$, $M_2$, $M_n$, 16, 17, 18, 20 (Figure 1).

**[0060]** The test data is provided from the internal test data output node 88 through the first NAND gate 76 to the external test data output terminal 82 only while the fuse element 70 is in its initial state.

**[0061]** Also, the test command input signal is provided from the external test command input terminal 84 to the internal test command input node 86 only while the fuse is in its initial state.

**[0062]** The second conductive layer $CN_2$ shields the fuse element 70, the inverters 72, 74, the resistor 75 and the NAND gates 76, 78 from direct external access.

**[0063]** The inverters 72, 74, the resistor 75 and the NAND gates 76, 78 are all coupled to the second conductive layer $CN_2$ so as to be powered by the power signal carried by the second conductive layer $CN_2$.

**[0064]** Additional protection is afforded by burying the signal paths from the fuse element 70 to the first and second NAND gates 76, 78 as far down into the chip 10 as possible to further preclude probe attacks. Therefore, the signal paths from the fuse element 70 to the first and second NAND gates 76, 78 are distributed primarily to an N+ or P+ diffusion. Polysilicon and other conductive layers may be used as well, with diminishing security. The use of the uppermost conductive layers $CN_n$ $CN_{n-1}$ should be avoided.

## Claims

1. An integrated circuit chip (10) containing a secure area (11) in which secure data is processed and/or stored, comprising

   a semiconductor layer (SC) containing diffusions (S,D) defining circuit element components;

   a first conductive layer ($CN_1$) coupled to the semiconductor layer to interconnect the components to thereby define circuit elements (14, 16, 17, 18, 20, $M_1$, $M_2$, $M_n$) for distributing, storing, processing and/or affecting the procesing of secure data;

   a second conductive layer ($CN_2$) overlying the circuit elements to thereby define a secure area (11) in which the circuit elements are shielded from inspection, and coupled to the circuit elements for conducting to the circuit elements a predetermined signal that is essential to an intended function of the circuit elements, whereby removal of the second conductive layer will prevent the predetermined essential signal from being provided to the circuit elements and thereby prevent the intended function;

   characterised in that the shielded circuit elements further comprise:

a fuse element (42, 57, 70) having an initial state and an irreversibly altered state; and

means (44, 58, 79) coupled to the fuse element for irreversibly altering the state of the fuse element in response to a predetermined control signal;
wherein the fuse element is coupled to another component of the chip such that irreversibly altering the state of the fuse element prevents some function of the chip.

2. An integrated circuit chip according to Claim 1, characterised in that the shielded circuit elements comprise means (60) for enabling said storage of secure data; and that the fuse element (56) is coupled to the enabling means so as to enable said secure data storage only prior to the state of the fuse element being irreversibly altered.

3. An integrated circuit chip according to Claim 1, further comprising:

means (78) for accessing said circuit elements for testing said circuit elements;
characterised by the fuse element (70) being coupled to the accessing means so as to enable said access for testing only prior to the state of the fuse element being irreversibly altered.

4. An integrated circuit chip according to Claim 1, characterised in that the shielded circuit elements comprise:

a given circuit element (M) that stores, processes or affects the processing of secure data; and
means coupled to the fuse element (42) and the given circuit element (M) for monitoring the state of the fuse element and for preventing the intended function of the given circuit element after the state of the fuse element has been irreversibly altered.

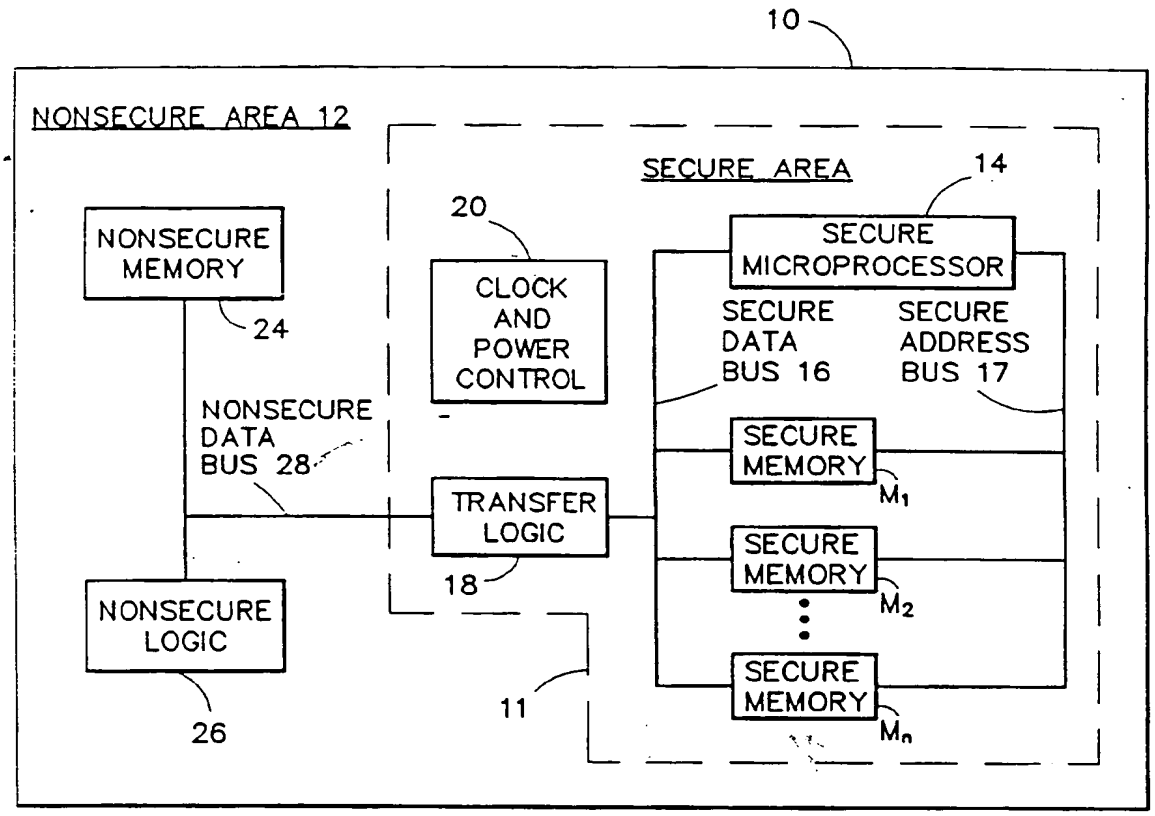


FIG. 1

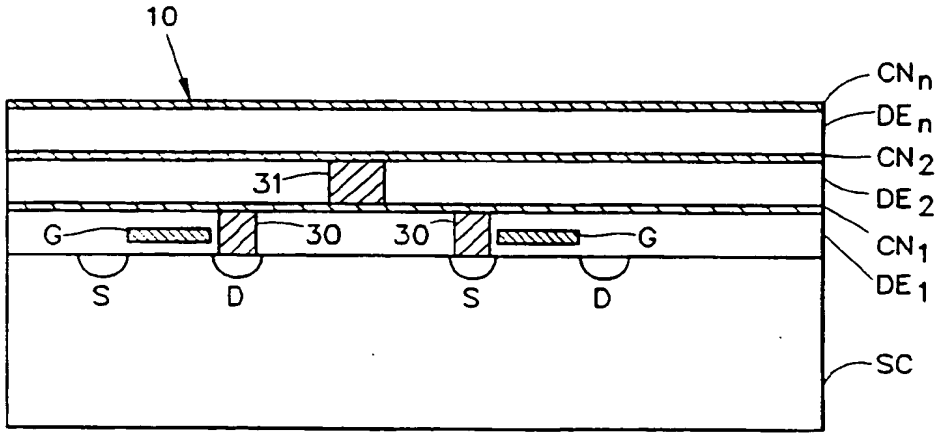


FIG. 2

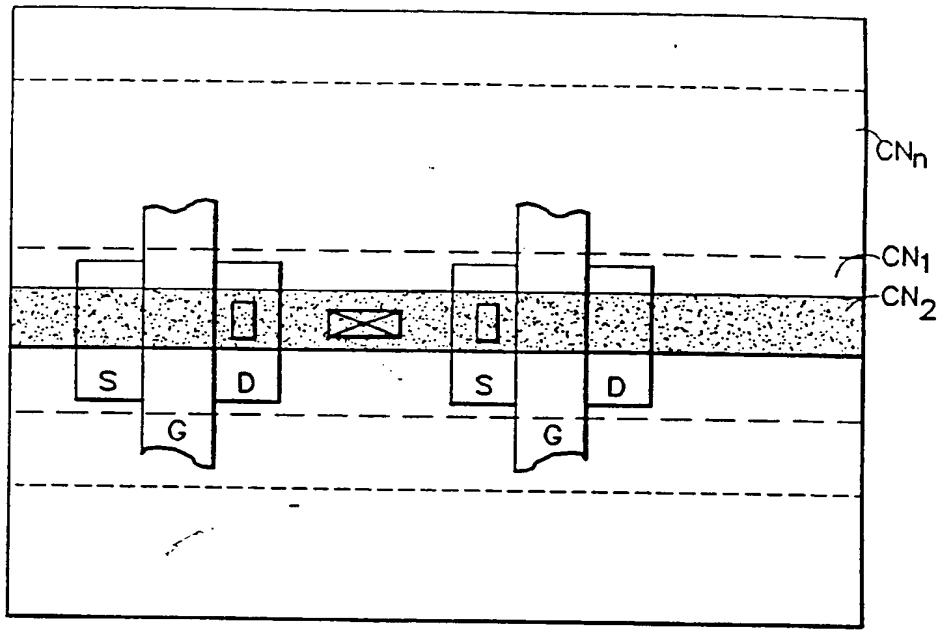


FIG. 3

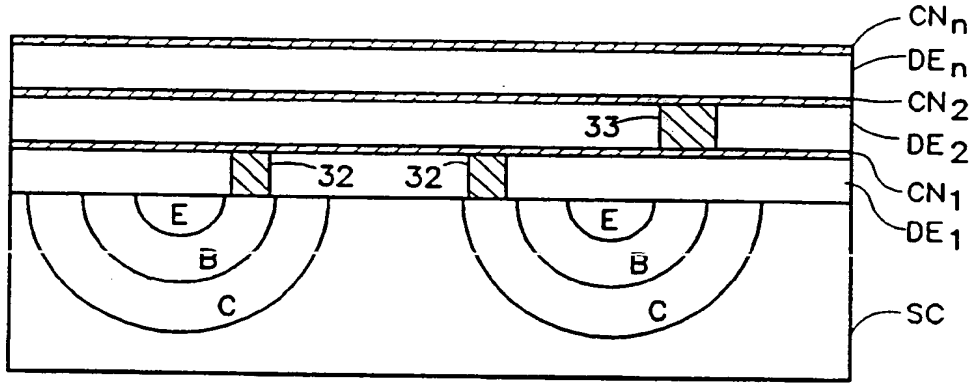


FIG. 4

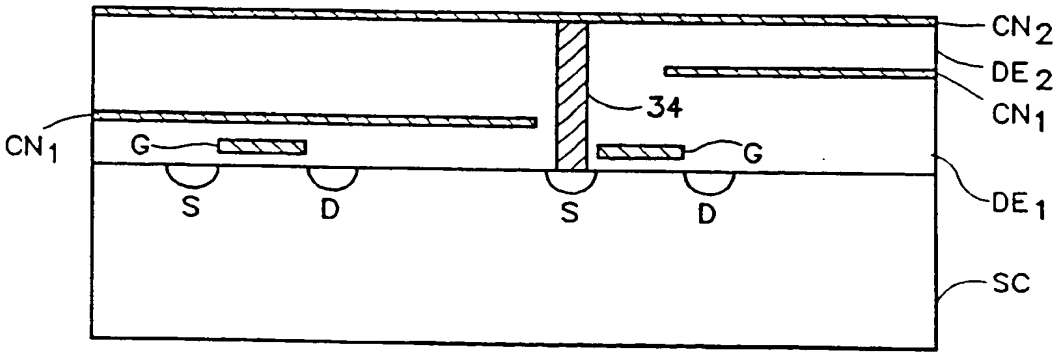


FIG. 5

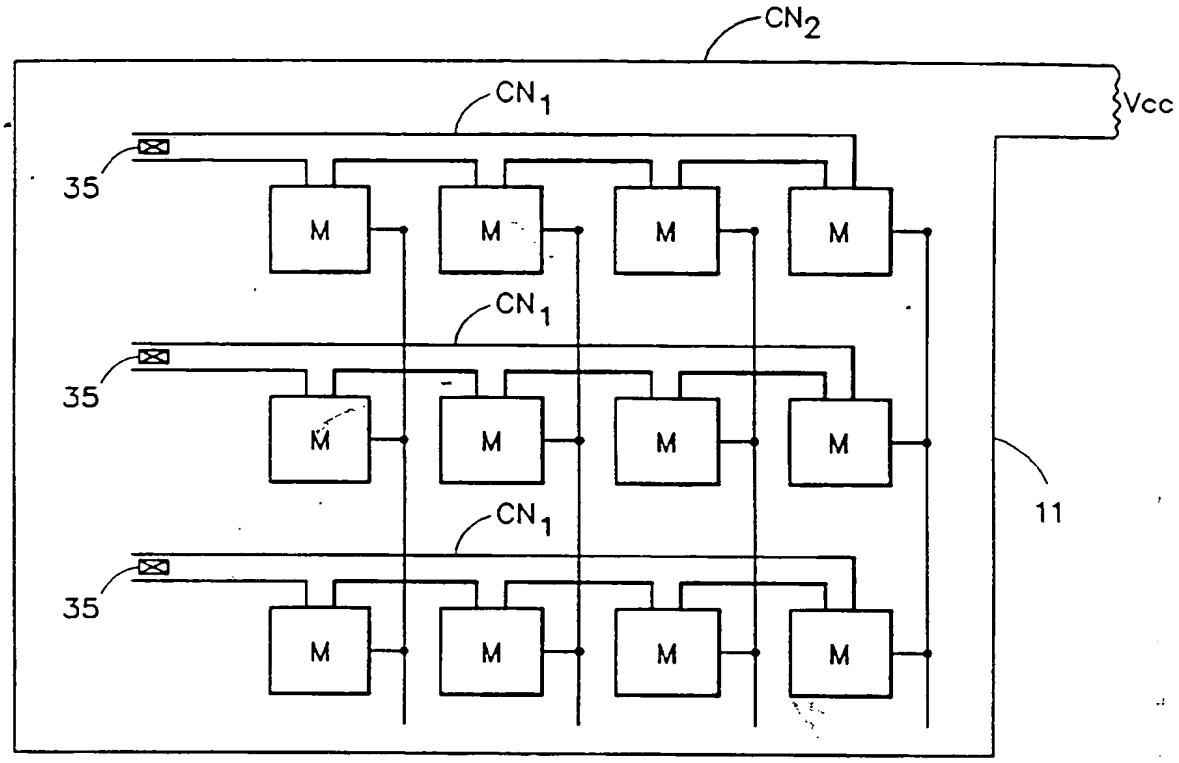


FIG. 6

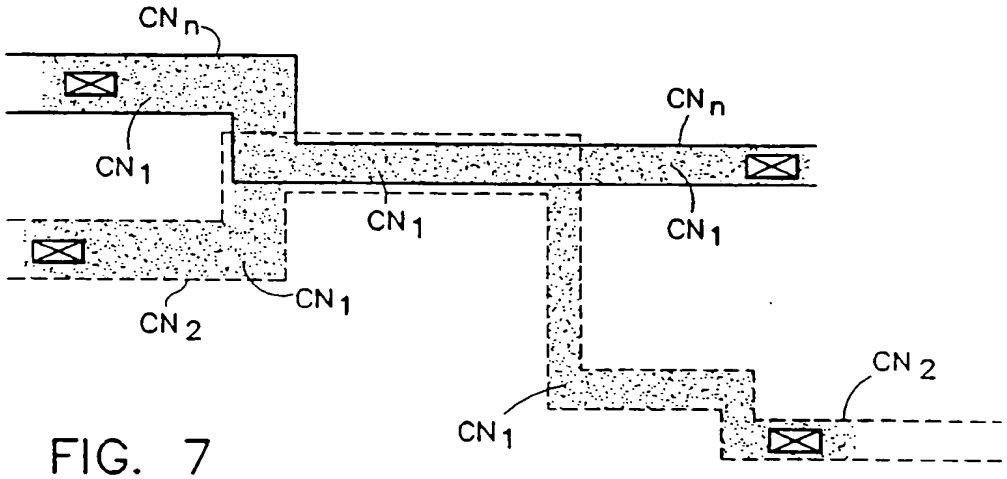


FIG. 7

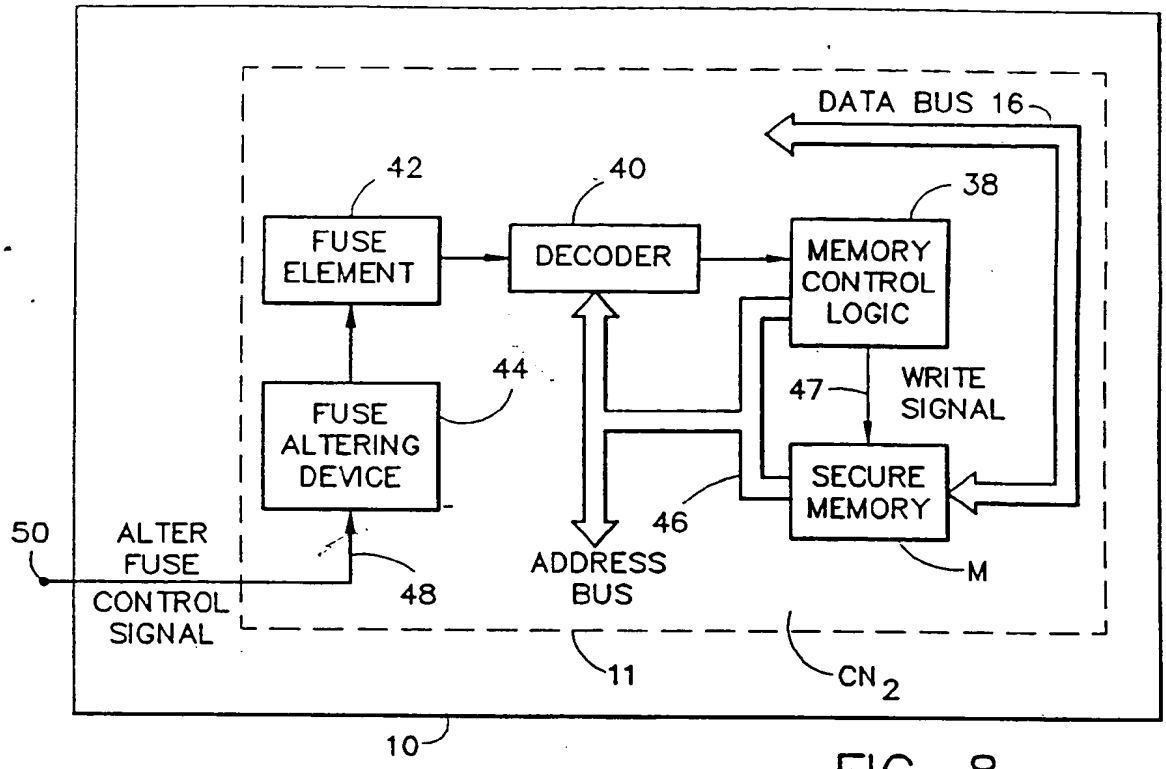


FIG. 8

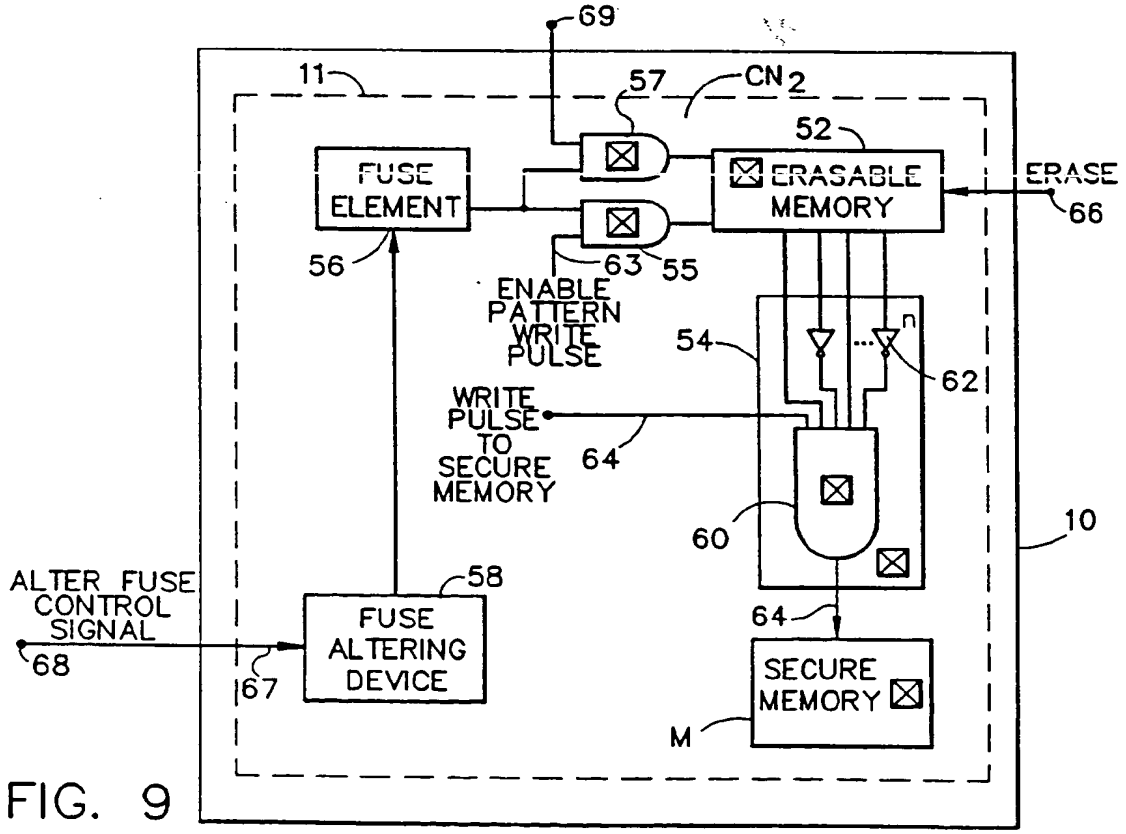


FIG. 9

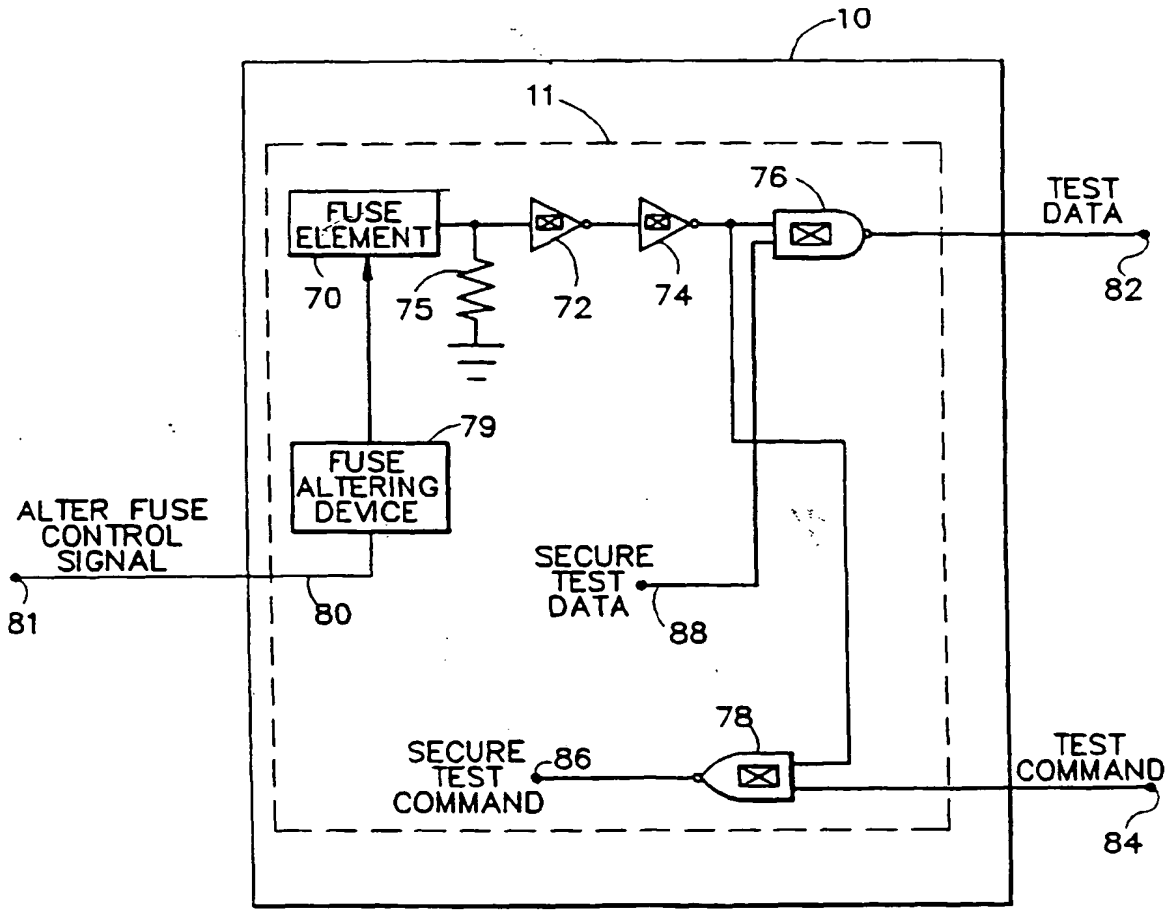


FIG. 10

(19) Eur päisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 920 057 A3

# (12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
**12.01.2000 Bulletin 2000/02**

(43) Date of publication A2:
**02.06.1999 Bulletin 1999/22**

(21) Application number: **99102130.4**

(22) Date of filing: **04.01.1990**

(51) Int. Cl.[7]: **H01L 23/58**, G11C 7/00

(84) Designated Contracting States:
**BE CH DE DK ES FR GB LI NL SE**

(30) Priority: **12.01.1989 US 297472**

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
**90300090.9 / 0 378 306**

(71) Applicant:
**General Instrument Corporation**
**Horsham, Pennsylvania 19044 (US)**

(72) Inventors:
- **Gilbert, Robert C**
  **San Diego, California 92131 (US)**
- **Knowles, Richard M**
  **Escondido, California 92026 (US)**
- **Moroney, Paul**
  **Olivenhain, California 92024 (US)**
- **Shumate, William allen**
  **Poway, California 92064 (US)**

(74) Representative:
**Blatchford, William Michael et al**
**Withers & Rogers**
**Goldings House,**
**2 Hays Lane**
**London SE1 2HW (GB)**

## (54) Secure integrated chip with conductive shield

(57) A chip includes a secure section 11 having a fuse element 56 and a fuse altering device 58. A predetermined data pattern is formed by wiring and inverters 62 connected between an erasable memory 52 and an AND gate 60. An enabling circuit 55 allows the predetermined data pattern to be written into the memory 52 when an appropriate control signal is received at a terminal 63. The state of the fuse element 56 is then irreversibly altered by the fuse altering device 58 so that the predetermined data pattern in the memory 52 cannot be changed. After final pressing and packaging, secure data may be stored in a secure memory M since the data pattern in the memory 52 is the same as that in the inverters 62. Once the secure data is stored, an erase signal is provided to terminal 66 which thereby erases the memory 52. The contents of the secure memory M are thereafter unalterable.

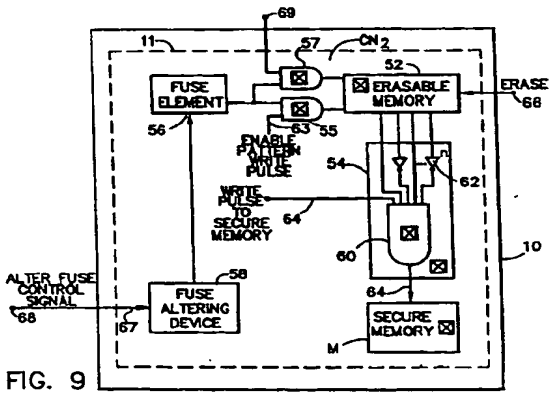


FIG. 9

EP 0 920 057 A3

European Patent Office

# EUROPEAN SEARCH REPORT

Application Number
EP 99 10 2130

## DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document with indication, where appropriate, of relevant passages | Relevant to claim | CLASSIFICATION OF THE APPLICATION (Int.Cl.6) |
|---|---|---|---|
| A | EP 0 169 941 A (SIEMENS AG)<br>5 February 1986 (1986-02-05)<br>* page 1, line 11 - line 30; figure A *<br>* page 4, line 7 - line 31; figures 2-4 * | 1 | H01L23/58<br>G11C7/00 |
| A | EP 0 221 351 A (SIEMENS AG)<br>13 May 1987 (1987-05-13)<br>* page 2, column 1, line 4 - line 27 *<br>* page 3, column 4, line 1 - line 40 *<br>* page 4, column 6, line 18 - page 5, column 7, line 36 * | 1 | |
| A | EP 0 172 108 A (EUROTECHNIQUE SA)<br>19 February 1986 (1986-02-19)<br>* abstract *<br>* page 1, line 1 - page 2, line 12 * | 1 | |
| A | GB 2 129 586 A (MCLAREN ROBERT ANDREW;PARKER CHARLES ROBERT CHRISTOP)<br>16 May 1984 (1984-05-16)<br>* page 4, line 38 - line 129; figure 3 * | 1 | |
| | | | TECHNICAL FIELDS SEARCHED (Int.Cl.6) |
| A | US 4 593 384 A (KLEIJNE THEODOOR A)<br>3 June 1986 (1986-06-03)<br>* the whole document * | 1 | H01L<br>G11C |
| A | US 3 882 323 A (SMOLKER GARY)<br>6 May 1975 (1975-05-06)<br>* the whole document * | 1 | |

The present search report has been drawn up for all claims

| Place of search | Date of completion of the search | Examiner |
|---|---|---|
| THE HAGUE | 18 November 1999 | Zeisler, P |

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

## ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 10 2130

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

18-11-1999

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| EP 0169941 A | 05-02-1986 | AT 47505 T | 15-11-1989 |
| | | JP 61042920 A | 01-03-1986 |
| | | US 4814849 A | 21-03-1989 |
| EP 0221351 A | 13-05-1987 | AT 67897 T | 15-10-1991 |
| | | DE 3681689 D | 31-10-1991 |
| | | HK 103693 A | 08-10-1993 |
| | | JP 2520857 B | 31-07-1996 |
| | | JP 62101050 A | 11-05-1987 |
| | | US 4941034 A | 10-07-1990 |
| EP 0172108 A | 19-02-1986 | FR 2569054 A | 14-02-1986 |
| | | US 4851894 A | 25-07-1989 |
| GB 2129586 A | 16-05-1984 | NONE | |
| US 4593384 A | 03-06-1986 | CA 1238716 A | 28-06-1988 |
| | | EP 0207126 A | 07-01-1987 |
| | | JP 62501242 T | 14-05-1987 |
| | | WO 8603861 A | 03-07-1986 |
| US 3882323 A | 06-05-1975 | NONE | |

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82